IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A method for authorizing an electronic data transfer for healthcare transactions comprising ~~the steps of~~:

receiving an authentication request containing a digital certificate from a requesting device via a communication link;

determining whether the digital certificate is valid;

creating an authentication response denying the authentication request when the digital certificate is not valid, or approving the authentication request when the digital certificate is valid;

sending the authentication response to the requesting device via the communication link; and

securely storing information about the electronic data transfer, the digital certificate and at least a portion of the authentication response such that non-repudiation of the electronic data transfer may be established.

Claim 2 (Original): The method as recited in claim 1 wherein the authentication request and the authentication response are transmitted via encrypted messages.

Claim 3 (Currently Amended): The method as recited in claim 1 wherein the step of determining whether the digital certificate is valid comprises ~~the steps of~~:

sending a validation request for the digital certificate to a validation authority; and

receiving a validation response from the validation authority indicating whether or not the digital certificate is valid.

Claim 4 (Original): The method as recited in claim 1 wherein the authentication response includes a date/time stamp.

Claim 5 (Original): The method as recited in claim 1 wherein the authentication response includes a digital receipt.

Claim 6 (Original): The method as recited in claim 5 wherein the digital receipt includes an identification of an originator of the electronic data transfer.

Claim 7 (Original): The method as recited in claim 5 wherein the digital receipt includes an identification of a recipient of the electronic data transfer.

Claim 8 (Original): The method as recited in claim 1 wherein the information about the electronic data transfer includes an electronic document.

Claim 9 (Currently Amended): A method for authorizing an electronic data transfer for healthcare transactions comprising ~~the steps of~~:

receiving an authentication request containing a digital certificate and information about the electronic data transfer from a requesting device via a communication link;

determining whether the digital certificate is valid;

creating an authentication response denying the authentication request when the digital certificate is not valid, or approving the authentication request when the digital certificate is valid;

sending the authentication response to the requesting device via the communication link;

creating a digital receipt for the electronic data transfer when the digital certificate is valid; and

securely storing the information about the electronic data transfer, the digital certificate and at least a portion of the authentication response such that non-repudiation of the electronic data transfer may be established.

Claim 10 (Original): The method as recited in claim 9 wherein the authentication request, the authentication response and the information about the electronic data transfer are transmitted via encrypted messages.

Claim 11 (Currently Amended): The method as recited in claim 9 wherein the step of determining whether the digital certificate is valid comprises ~~the steps of~~:

sending a validation request for the digital certificate to a validation authority; and

receiving a validation response from the validation authority indicating whether or not the digital certificate is valid.

Claim 12 (Original): The method as recited in claim 9 wherein the digital receipt includes a date/time stamp.

Claim 13 (Original): The method as recited in claim 9 wherein the digital receipt includes an identification of an originator of the electronic data transfer.

Claim 14 (Original): The method as recited in claim 9 wherein the digital receipt includes an identification of a recipient of the electronic data transfer.

Claim 15 (Original): The method as recited in claim 9 wherein the digital receipt includes an action taken relating to the electronic data transfer.

Claim 16 (Original): The method as recited in claim 9 wherein the information about the electronic data transfer includes an electronic document.

Claim 17 (Currently Amended): A computer program embodied on a computer readable medium for authorizing an electronic data transfer for healthcare transactions comprising:

a code segment for receiving an authentication request containing a digital certificate from a requesting device via a communication link;

a code segment for determining whether the digital certificate is valid;

a code segment for creating an authentication response denying the authentication request when the digital certificate is not valid, or approving the authentication request when the digital certificate is valid;

a code segment for sending the authentication response to the requesting device via the communication link; and

a code segment for securely storing information about the electronic data transfer, the digital certificate and at least a portion of the authentication response such that non-repudiation of the electronic data transfer may be established.

Claim 18 (Original): The computer program as recited in claim 17 wherein the authentication request and the authentication response are transmitted via encrypted messages.

Claim 19 (Original): The computer program as recited in claim 17 wherein the a code segment for determining whether the digital certificate is valid comprises:

a code segment for sending a validation request for the digital certificate to a validation authority; and

a code segment for receiving a validation response from the validation authority indicating whether or not the digital certificate is valid.

Claim 20 (Original): The computer program as recited in claim 17 wherein the authentication response includes a date/time stamp.

Claim 21 (Original): The computer program as recited in claim 17 wherein the authentication response includes a digital receipt.

Claim 22 (Original): The computer program as recited in claim 21 wherein the digital receipt includes an identification of an originator of the electronic data transfer.

Claim 23 (Original): The computer program as recited in claim 21 wherein the digital receipt includes an identification of a recipient of the electronic data transfer.

Claim 24 (Original): The computer program as recited in claim 17 wherein the information about the electronic data transfer includes an electronic document.

Claim 25 (Currently Amended): A computer program embodied on a computer readable medium for authorizing an electronic data transfer for healthcare transactions comprising:

a code segment for receiving an authentication request containing a digital certificate and information about the electronic data transfer from a requesting device via a communication link;

a code segment for determining whether the digital certificate is valid;

a code segment for creating an authentication response denying the authentication request when the digital certificate is not valid, or approving the authentication request when the digital certificate is valid;

a code segment for sending the authentication response to the requesting device via the communication link;

a code segment for creating a digital receipt for the electronic data transfer when the digital certificate is valid; and

a code segment for securely storing the information about the electronic data transfer, the digital certificate and at least a portion of the authentication response such that non-repudiation of the electronic data transfer may be established.

Claim 26 (Original): The computer program as recited in claim 25 wherein the authentication request, the authentication response and the information about the electronic data transfer are transmitted via encrypted messages.

Claim 27 (Original): The computer program as recited in claim 25 wherein the a code segment for determining whether the digital certificate is valid comprises:

a code segment for sending a validation request for the digital certificate to a validation authority; and

a code segment for receiving a validation response from the validation authority indicating whether or not the digital certificate is valid.

Claim 28 (Original): The computer program as recited in claim 25 wherein the digital receipt includes a date/time stamp.

Claim 29 (Original): The computer program as recited in claim 25 wherein the digital receipt includes an identification of an originator of the electronic data transfer.

Claim 30 (Original): The computer program as recited in claim 25 wherein the digital receipt includes an identification of a recipient of the electronic data transfer.

Claim 31 (Original): The computer program as recited in claim 25 wherein the digital receipt includes an action taken relating to the electronic data transfer.

Claim 32 (Original): The computer program as recited in claim 25 wherein the information about the electronic data transfer includes an electronic document.

Claim 33 (Currently Amended): A system for authorizing an electronic data transfer <u>for healthcare transactions</u> comprising:

a computer;

a data storage device communicably linked to the computer;

a requesting device communicably linked to the computer; and

the computer receiving an authentication request containing a digital certificate from the requesting device, determining whether the digital certificate is valid, creating an authentication response denying the authentication request when the digital certificate is not valid, or approving the authentication request when the digital certificate is valid, sending the authentication response to the requesting device, and securely storing information about the electronic data transfer, the digital certificate and at least a portion of the authentication response on the data storage device such that non-repudiation of the electronic data transfer may be established.

Claim 34 (Original): The system as recited in claim 33 wherein the authentication request and the authentication response are transmitted via encrypted messages.

Claim 35 (Currently Amended): The system as recited in claim 33 further comprising:

a validation authority communicably linked to the computer via a second communication link; and

the computer determining whether the digital certificate is valid by sending a validation request for the digital certificate to [[a]] the validation authority, and receiving a validation response from the validation authority indicating whether or not the digital certificate is valid.

Claim 36 (Original): The system as recited in claim 33 wherein the authentication response includes a date/time stamp.

Claim 37 (Original): The system as recited in claim 33 wherein the authentication response includes a digital receipt.

Claim 38 (Original): The system as recited in claim 37 wherein the digital receipt includes an identification of an originator of the electronic data transfer.

Claim 39 (Original): The system as recited in claim 37 wherein the digital receipt includes an identification of a recipient of the electronic data transfer.

Claim 40 (Original): The system as recited in claim 33 wherein the information about the electronic data transfer includes an electronic document.

Claim 41 (Currently Amended): A system for authorizing an electronic data transfer for healthcare transactions comprising:

a computer;

a data storage device communicably linked to the computer;

a requesting device communicably linked to the computer; and

the computer receiving an authentication request containing a digital certificate and information about the electronic data transfer from the requesting device, determining whether the digital certificate is valid, creating an authentication response denying the authentication request when the digital certificate is not valid, or approving the authentication request and creating a digital receipt for the electronic data transfer when the digital certificate is valid, sending the authentication response to the requesting device, and securely storing the information about the electronic data transfer, the digital certificate and at least a portion of the authentication response on the data storage device such that non-repudiation of the electronic data transfer may be established.

Claim 42 (Original): The system as recited in claim 41 wherein the authentication request, the authentication response and the information about the electronic data transfer are transmitted via encrypted messages.

Claim 43 (Original): The system as recited in claim 41 further comprising:

a validation authority communicably linked to the computer via a second communication link; and

the computer determining whether the digital certificate is valid by sending a validation request for the digital certificate to a validation authority, and receiving a validation response from the validation authority indicating whether or not the digital certificate is valid.

Claim 44 (Original): The system as recited in claim 41 wherein the digital receipt includes a date/time stamp.

Claim 45 (Original): The system as recited in claim 41 wherein the digital receipt includes an identification of an originator of the electronic data transfer.

Claim 46 (Original): The system as recited in claim 41 wherein the digital receipt includes an identification of a recipient of the electronic data transfer.

Claim 47 (Original): The system as recited in claim 41 wherein the digital receipt includes an action taken relating to the electronic data transfer.

Claim 48 (Original): The system as recited in claim 41 wherein the information about the electronic data transfer includes an electronic document.